UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

ERICA JUDKA, individually and on behalf of all others similarly situated, Plaintiff, v. RITE AID CORPORATION, Defendant.	Case No. **COMPLAINT – CLASS ACTION** JURY TRIAL DEMANDED

Plaintiff Erica Judka ("Plaintiff"), individually and on behalf of all others similarly situated, by and through the undersigned attorneys, brings this class action against Defendant Rite Aid Corporation, ("Rite Aid" or "Defendant") and complains and alleges upon personal knowledge and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Rite Aid for its failure to secure and safeguard Plaintiff's and approximately 2.2 million other individuals' personally identifiable information, including names, dates of birth, drivers' license numbers, and other forms of government issued IDs (collectively, "PII").

2. Defendant Rite Aid is a Philadelphia-based, Fortune 500 drugstore chain that operates more than 1,700 retail pharmacy locations across 16 states.[1]

[1] https://news.riteaid.com/about-us/history/default.aspx (last accessed July 18, 2024).

3. In data breach notification letters filed with the Office of Maine's Attorney General, Rite Aid stated it detected the incident on June 6, 2024, 12 hours after the attackers breached its network using an employee's credentials.[2]

4. Rite Aid "determined by June 17, 2024, that certain data associated with the purchase or attempted purchase of specific retail products was *acquired* by the unknown third party. This data included purchaser name, address, date of birth and driver's license number or other form of government-issued ID presented at the time of a purchase between June 6, 2017, and July 30, 2018."[3] (the "Data Breach").

5. Rite Aid provided limited details about the Data Breach, including whether or not the cybercriminal(s) responsible for breach were identified or whether the information exfiltrated was held for ransom. Rite Aid also did not disclose whether its investigation detected the compromised information on the dark web. Rite Aid simply offered access to credit monitoring and identity restoration services through Kroll at no charge to affected individuals but, as Plaintiff's allegations will make clear, this offer is woefully inadequate.

6. Rite Aid's Notice did not disclose how it discovered the Data Breach, the means and mechanism of the cyberattack, and, importantly, what specific steps Rite Aid took following the Data Breach to secure its systems and prevent future cyberattacks.

7. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect PII from the foreseeable threat of a cyberattack.

[2] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/c4bace65-85df-4fff-b99f-f8fd390bb41a.html (last accessed July 18, 2024).
[3] *Id.* (emphasis added).

8. By being entrusted with Plaintiff's and Class Members' PII for its own pecuniary benefit, Defendant assumed a duty to Plaintiff and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiff's and Class Members' PII against unauthorized access and disclosure. Defendant also had a duty to adequately safeguard this PII under applicable law, as well as pursuant to industry standards and duties imposed by statutes, including Section 5 of the Federal Trade Commission Act ("FTC Act"). Defendant breached those duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the PII in its possession from unauthorized access and disclosure.

9. As a result of Defendant's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff and approximately 2.2 million Class Members suffered injury and ascertainable losses in the form of out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, the diminution in value of their personal information from the exposure, and the present and imminent thread of fraud and identity theft. This action seeks to remedy these failings and their consequences.

10. Rite Aid's failure to timely notify the victims of its Data Breach meant that Plaintiff and Class Members were unable to immediately take affirmative measures to prevent or mitigate the resulting harm.

11. Despite having been accessed and "acquired" by unauthorized criminal actors, Plaintiff's and Class Members' sensitive and confidential PII remains in the possession of Defendant. Absent additional safeguards and independent review and oversight, the information remains vulnerable to further cyberattacks and theft.

12. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to adequately train its staff and employees on proper security measures; and failing to provide Plaintiff and Class Members with prompt and adequate notice of the Data Breach.

13. In addition, Defendant failed to properly monitor the network and systems that housed the PII. Had Defendant properly monitored these electronic systems, it would have discovered the intrusion sooner or prevented it altogether.

14. The security of Plaintiff's and Class Members' identities has long been and remains at risk because of Defendant's wrongful conduct, as the PII that Defendant collected and maintained is now in the hands of data thieves. This present risk will continue for the course of their lives.

15. Armed with the PII accessed in the Data Breach, data thieves can commit a wide range of crimes including, for example, opening new financial accounts in Class Members' names, taking out loans in their names, using their identities to obtain government benefits, filing fraudulent tax returns using their information, and giving false information to police during an arrest.

16. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Among other measures, Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft. Further, Plaintiff and Class Members will incur out-of-pocket costs to purchase

adequate credit monitoring and identity theft protection and insurance services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

17. Plaintiff and Class Members will also be forced to expend additional time to review credit reports and monitor their financial accounts for fraud or identity theft. Moreover, because the exposed information includes drivers' license numbers, government ID information, and other immutable personal details, the risk of identity theft and fraud will persist throughout their lives.

18. Plaintiff and Class Members seek to hold Defendant responsible for the harms resulting from the massive and preventable disclosure of such sensitive and personal information. Plaintiff seeks to remedy the harms resulting from the Data Breach on behalf of herself and all similarly situated individuals whose PII was accessed and exfiltrated during the Data Breach.

19. Plaintiff, individually and on behalf of all other Class Members, brings claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, breach of confidence, and for declaratory and injunctive relief. To remedy these violations of law, Plaintiff and Class Members seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to Rite Aid's data security protocols and employee training practices); reasonable attorneys' fees, costs, and expenses incurred in bringing this action; and all other remedies the Court deems just and proper.

PARTIES

Plaintiff

Plaintiff Erica Judka

20. Plaintiff Judka is a resident and citizen of the Commonwealth of Pennsylvania. Plaintiff provided PII, or otherwise had PII provided to, Rite Aid in connection with transacting with Rite Aid. On July 15, 2024, Rite Aid sent, and Plaintiff received, a letter indicating that her

information was impacted by the Data Breach, including Plaintiff's name, address, date of birth, and driver's license number or other form of government identification. The letter confirmed that Plaintiff's exposed information was in connection with purchases made between June 6, 2017 and July 30, 2018.

21. After Plaintiff received the notice letter, she checked her bank statements for fraud.

22. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff will need to maintain these heightened measures for years.

23. Plaintiff also suffered actual injury from having PII compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of Plaintiff's confidential PII—a form of property that Plaintiff entrusted to Rite Aid, which was compromised as a result of the Data Breach it failed to prevent and (b) a violation of Plaintiff's privacy rights as a result of Rite Aid's unauthorized disclosure of PII.

24. As a result of Rite Aid's failure to adequately safeguard Plaintiff's information, Plaintiff has been injured. Plaintiff has experienced an uptick in spam calls and robocalls since shortly after the Data Breach. Plaintiff is also at a continued risk of harm because the PII remains in Rite Aid's systems, which have already been shown to be susceptible to compromise and attack, and is subject to further attack so long as Rite Aid fails to undertake the necessary and appropriate data security measures to protect the PII in its possession.

Defendant

25. Defendant Rite Aid Corporation is a Delaware corporation with its principal office or place of business located at 1200 Intrepid Ave., 2nd Floor, Philadelphia, Pennsylvania. It conducts business through several wholly owned subsidiaries. Rite Aid Corporation transacts or

has transacted business routinely in this District and throughout the United States.

JURISDICTION AND VENUE

26. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

27. This Court has personal jurisdiction over Rite Aid because Rite Aid maintains its principal place of business in Pennsylvania and conducts substantial business in Pennsylvania and in this District through its principal place of business; engaged in the conduct at issue herein from and within this District; and otherwise has substantial contacts with this District and purposely availed itself of the Courts in this District.

28. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) and (2) because Rite Aid resides in this District, and this District is where a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred.

FACTUAL ALLEGATIONS

Overview of Rite Aid Corporation and Collection of PII

29. Founded in 1962 in Scranton, Rite Aid is a national drugstore chain based in Philadelphia. Rite Aid is headquartered in Penns Landing in Philadelphia, Pennsylvania.

30. In the regular course of its business, Rite Aid collects and maintains highly sensitive PII of consumers. As a regular and necessary part of its business, Rite Aid collects and maintains sensitive PII from its customers, which is obtained and used in connection with in-store transactions. That information includes, but is not limited to, names, dates of birth, driver's license numbers, and other government ID numbers. Rite Aid stores this information digitally.

31. Rite Aid is and was aware of the sensitive nature of the PII it collects, and it acknowledges the importance of data privacy. Indeed, in its Privacy Policy on its website, Rite Aid claims that it "respects your concerns about privacy."[4]

32. By obtaining, collecting, using, and benefitting from Plaintiff's and Class Member's PII, Defendant assumed legal and equitable duties that required Defendant to, at a minimum, implement adequate safeguards to prevent unauthorized use or disclosure of PII and to report any unauthorized use or disclosure of PII.

The Data Breach

33. In data breach notification letters filed with the Office of Maine's Attorney General, Rite Aid disclosed that it detected the Data Breach on June 6, 2024, 12 hours after the attackers breached its network using an employee's credentials.[5]

34. Per its notices, Rite Aid "determined by June 17, 2024, that certain data associated with the purchase or attempted purchase of specific retail products was *acquired* by the unknown third party. This data included purchaser name, address, date of birth and driver's license number or other form of government-issued ID presented at the time of a purchase between June 6, 2017, and July 30, 2018."[6] (the "Data Breach").

35. Despite learning of the Data Breach as early as June 2024, Rite Aid did not announce the Data Breach publicly until July 2024 and did not begin sending out Data Breach notification letters to affected individuals until around that time.

36. Rite Aid provided limited details about the Data Breach, including whether or not the cybercriminal(s) responsible for breach were identified or whether the information exfiltrated

[4] https://www.RiteAid-inc.com/privacy-policy/ (last accessed May 2, 2024).
[5] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/c4bace65-85df-4fff-b99f-f8fd390bb41a.html (last accessed July 18, 2024).
[6] *Id.* (emphasis added).

was held for ransom. Rite Aid also did not disclose whether its investigation detected the compromised information on the dark web. Instead, Rite Aid simply offered access to credit monitoring and identity restoration services through Kroll.

37. Rite Aid's Notice omits pertinent information including how criminals gained access to the files on its systems, what computer systems were impacted, the means and mechanisms of the cyberattack, the reason for the delay in notifying Plaintiff and Class Members of the Data Breach, how it determined that the PII had been accessed, and of particular importance to Plaintiff and Class Members, the actual steps Rite Aid took following the Data Breach to secure its systems and train its employees to prevent further cyberattacks.

38. Based on Rite Aid's acknowledgments, it is evident that unauthorized criminal actors did in fact access Rite Aid's network and exfiltrated Plaintiff's and Class Members' PII in an attack designed to acquire that sensitive, confidential, and valuable information.

39. The PII contained in the files accessed by cybercriminals appears not to have been encrypted because if properly encrypted, the attackers would have acquired unintelligible data and would not have accessed Plaintiff's and Class Members' PII.

40. The Data Breach reportedly impacted the PII of approximately 2.2 million individuals.

Rite Aid Failed to Follow FTC Guidelines

41. Defendant was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair

practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

42. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

43. According to the FTC, the need for data security should be factored into all business decision-making.

44. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.

45. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

46. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

47. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

48. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

49. Defendant failed to properly implement basic data security practices.

50. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to individuals' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

51. Defendant was at all times fully aware of its obligation to protect its customers' and employees' PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Rite Aid Failed to Comply with Industry Standards for Data Security

52. Experts studying cybersecurity routinely identify corporations as being particularly vulnerable to cyberattacks because of the value of the PII that these entities collect and maintain.

53. Several best practices have been identified that at a minimum should be implemented by corporate entities like Defendant, including, but not limited to: educating all employees; strong passwords; multi-layer security, such as firewalls and anti-virus and anti-malware software; encryption (e.g., making data unreadable without a key); multi-factor authentication; backup data; and limiting the number of employees with access to sensitive data.

54. Other standard best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers;

monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

55. Defendant failed to meet the minimum standards of, e.g., the NIST Cybersecurity Framework, and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established industry standards in reasonable cybersecurity readiness.

56. These foregoing frameworks are existing and applicable industry standards in the corporate sector and Defendant failed to comply with these accepted standards, thereby opening the door to cybercriminals and causing the Data Breach.

Rite Aid Owed Plaintiff and Class Members a Duty to Safeguard Their PII

57. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Plaintiff and Class Members.

58. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including adequately training its employees and others who accessed PII within its computer systems on how to adequately protect PII.

59. Defendant owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of PII in a timely manner.

60. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

61. Defendant owed a duty to Plaintiff and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

62. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of inadequate data security practices.

Rite Aid Knew That Criminals Target PII

63. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in industries holding significant amounts of PII preceding the date of the breach.

64. At all relevant times, Defendant knew, or should have known, that Plaintiff's and all other Class Members' PII was a target for malicious actors. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' PII from cyberattacks that Defendant should have anticipated and guarded against.

65. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the PII belonging to Rite Aid's consumers, like Plaintiff and Class Members.

66. PII is a valuable property right.[7] The value of PII as a commodity is measurable.[8] "Firms are now able to attain significant market valuations by employing business models

[7] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP Advances in Information and Communication Technology (May 2015), https://www.researchgate.net/publication/283668023 ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...").

[8] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, Medscape (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

predicated on the successful use of personal data within the existing legal and regulatory frameworks."[9] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[10] Personal data is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

67. As a result of its real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, driver's license numbers, other ID numbers, Social Security numbers, PII, and other sensitive information directly on various websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

68. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[11]

69. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[9] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, No. 220, p.4, OECD Publishing (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[10] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, Interactive Advertising Bureau (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[11] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) Information Systems Research 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

70. Indeed, cyberattacks have been common for over ten years with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[12]

71. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[13]

72. The Office for Civil Rights ("OCR") urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, OCR's deputy director of health information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[14]

Theft of PII has Grave and Lasting Consequences for Victims

---

[12] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

[13] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[14] *Stolen Laptops Lead to Important HIPAA Settlements*, U.S. Department of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

73. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[15]

74. Identity thieves use PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[16] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or other form of identification, and/or use the victim's information in the event of arrest or court action.[17]

75. With access to an individual's PII, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture, obtaining government benefits, or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's information, rent a house, or receive medical

---

[15] *See What to Know About Identity Theft*, Federal Trade Commission Consumer Advice, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed on Jan. 25, 2024).

[16] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[17] Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, Experian (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[18]

76. Each year, identity theft causes billions of dollars of losses to victims in the United States. For example, with the PII stolen in the Data Breach, which includes drivers' license numbers and government ID numbers, identity thieves can open financial accounts, apply for credit, commit financial crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members.

77. Personally identifiable information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use the information and trade it on dark web black-markets for years to come.

78. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.

79. The PII exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending and substantial. As the FTC has reported, if cyberthieves get access to a person's highly sensitive information, they will use it.[19]

---

[18] *See Warning Signs of Identity Theft*, Federal Trade Commission, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited May 2, 2024).

[19] Ari Lazarus, *How fast will identity thieves use stolen info?*, Federal Trade Commission (May 24, 2017), available at https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info.

80. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information . . . are worth more than 10x on the black market."[20]

81. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[21]

82. Theft of drives' license numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced.

83. Due to their highly sensitive nature, theft of drivers' license numbers in combination with other PII (e.g., name, address, date of birth) can result in a variety of fraudulent activity.

84. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later.

85. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[22]

---

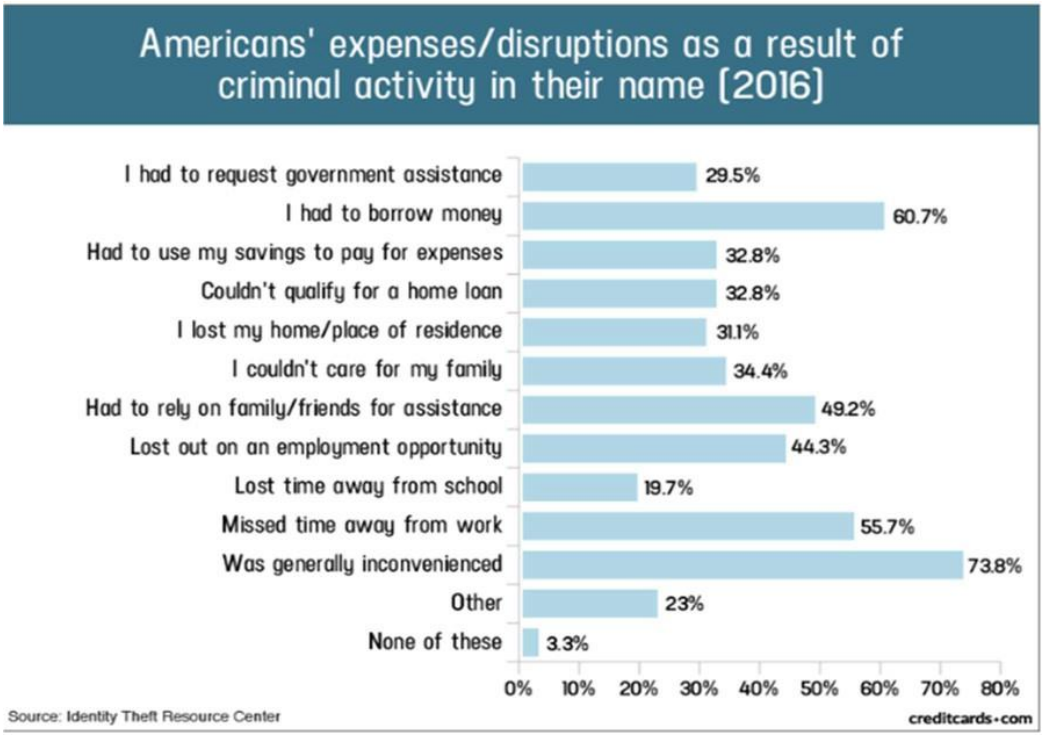
[20] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), https://www.redseal.net/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers/

[21] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces*, Identity Theft Resource Center (2021), accessible at https://www.idtheftcenter.org/identity-theft-aftermath-study/.

[22] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

86. It is within this context that Plaintiff and all other Class Members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

87. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:



88. Victims of the Data Breach, like Plaintiff and Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[23]

89. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud

[23] *Guide for Assisting Identity Theft Victims*, Federal Trade Commission, 4 (Sept. 2013), http://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

and identity theft. Plaintiff and Class Members must now m the time and expend the effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and other account information for unauthorized activity for years to come.

90. Plaintiff and Class Members have suffered or will suffer actual harms for which they are entitled to compensation, including, but not limited to the following:

a. Trespass, damage to, and theft of their personal property, including PII;

b. Improper disclosure of their PII;

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their PII being in the hands of criminals and having already been misused;

d. The imminent and certainly impending risk of having their confidential PII used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class Members' PII for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PII; and

k. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

91. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which remains in the possession of Defendant, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendant has shown to be incapable of protecting Plaintiff's and Class Members' PII.

The Data Breach was Foreseeable and Preventable

92. Data disclosures and data breaches are preventable.[24] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[25] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised "[26]

93. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[27]

[24] Lucy L. Thompson, *Despite the Alarming Trends, Data Breaches Are Preventable*, Data Breach and Encryption Handbook (Lucy Thompson, ed., 2012).
[25] *Id.* at 17.
[26] *Id.* at 28.
[27] *Id.*

94. As explained by the FBI, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[28]

95. Plaintiff and Class Members entrusted their PII to Defendant as a condition of transacting business with and at Rite Aid. Plaintiff and Class Members understood and expected that Defendant or anyone in Defendant's position would safeguard their PII against cyberattacks, delete or destroy PII that Defendant was no longer required to maintain, and timely and accurately notify them if their PII was compromised.

Damages Sustained by Plaintiff and Class Members

96. To date, Defendant has done nothing to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach. Rite Aid only offered credit monitoring through Kroll, but did not disclose how it determined eligibility. Not only did Defendant fail to provide adequate ongoing credit monitoring or identity protection services for individuals impacted by the Data Breach, but the credit monitoring identity theft protection services does nothing to compensate Plaintiff and Class Members for damages incurred, and time spent dealing with, the Data Breach.

97. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

98. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and Class Members face substantial risk of out-of-pocket fraud

[28] *See How to Protect Your Networks from RANSOMWARE*, at 3, FBI.gov, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed May 2, 2024).

losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

99. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

100. Plaintiff and Class Members have and will also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

101. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions and/or government agencies to dispute unauthorized and fraudulent activity in their names;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

102. Plaintiff and Class Members suffered actual injury from having their PII compromised as a result of the Data Breach including, but not limited to: (a) damage to and

diminution in the value of their PII, a form of property that Rite Aid obtained from Plaintiff and Class Members; (b) violation of their privacy rights; (c) imminent and impending injury arising from the increased risk of identity theft and fraud; and (d) emotional distress.

103. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy with respect to that information.

104. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at a present and imminent and increased risk of future harm.

105. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing PII is not accessible online, is properly encrypted, and that access to such data is password protected.

106. Many failures laid the groundwork for the occurrence of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cybersecurity training, procedures, and protocols that were necessary to protect Plaintiff's and Class Members' PII.

107. Defendant maintained the PII in an objectively reckless manner, making the PII vulnerable to unauthorized disclosure.

108. Defendant knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would result if Plaintiff's and Class

Members' PII were stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of the breach.

109. The risk of improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and Defendant was on notice that failing to take necessary steps to secure Plaintiff's and Class Members' PII from that risk left the PII in a dangerous condition.

110. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their PII was protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members with prompt and accurate notice of the Data Breach.

CLASS ALLEGATIONS

111. Plaintiff brings this class action individually and on behalf of all members of the following class of similarly situated persons pursuant to Federal Rule of Civil Procedure 23:

Nationwide Class

All persons in the United States whose PII was compromised in the Data Breach disclosed by Rite Aid, including all persons who were sent notice of the Data Breach.

112. Alternatively, or in addition to the nationwide class, Plaintiff seeks to represent the following subclass:

Pennsylvania Subclass

All persons in the Commonwealth of Pennsylvania whose PII was compromised in the Data Breach disclosed by Rite Aid, including all persons who were sent notice of the Data Breach.

113. The nationwide class and the Pennsylvania Subclass are collectively referred to as the "Class." Excluded from the Class are Rite Aid and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

114. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of Plaintiff's claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

115. Numerosity: The members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable. As noted above, approximately 2.2 million individuals' information was exposed in the Data Breach.

116. Commonality and Predominance: Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class Members. Such common questions of law or fact include, *inter alia*:

a. Whether Rite Aid had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' PII from unauthorized access and disclosure;

b. Whether they computer systems and data security practices employed by Rite Aid to protect Plaintiff's and Class Members' PII violated the FTC Act, and/or state laws and/or Rite Aid's other duties discussed herein;

c. Whether Rite Aid failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and Class Members;

d. Whether Plaintiff and Class Members suffered injury as a proximate result of Rite Aid's negligent actions or failures to act;

e. Whether Rite Aid failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' PII;

f. Whether an implied contract existed between Class Members and Rite Aid providing that Rite Aid would implement and maintain reasonable security measures to protect and secure Class Members' PII from unauthorized access and disclosure;

g. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and Class Members;

h. Whether Rite Aid's actions and inactions alleged herein constitute gross negligence;

i. Whether Rite Aid breached its duties to protect Plaintiff's and Class Members' PII; and

j. Whether Plaintiff and all other members of the Class are entitled to damages and the measure of such damages and relief.

117. Rite Aid engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

118. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had PII compromised in the Data Breach. Plaintiff and Class

Members were injured by the same wrongful acts, practices, and omissions committed by Rite Aid, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

119. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class Members. Plaintiff is an adequate representative of the Class and has no interests adverse to, or in conflict with, the Class that Plaintiff seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

120. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and all other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Rite Aid, so it would be impracticable for Class Members to individually seek redress from Rite Aid's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the Class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I
NEGLIGENCE

121. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

122. Rite Aid owed a duty to Plaintiff and all other Class Members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

123. Rite Aid knew, or should have known, the risks of collecting and storing Plaintiff's and Class Members' PII and the importance of maintaining secure systems. Rite Aid knew, or should have known, of the many data breaches that targeted companies holding significant amounts of PII in recent years.

124. Given the nature of Rite Aid's business, the sensitivity and value of the PII it maintains, and the resources at its disposal, Rite Aid should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

125. Rite Aid breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiff's and Class Members' PII.

126. It was reasonably foreseeable to Rite Aid that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

127. But for Rite Aid's negligent conduct or breach of the above-described duties owed to Plaintiff and Class Members, their PII would not have been compromised.

128. As a result of Rite Aid's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II
NEGLIGENCE PER SE

129. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

130. Rite Aid's duties arise from, *inter alia*, Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by businesses, such as Rite Aid, of failing to employ reasonable measures to protect and secure PII.

131. Plaintiff and Class Members are within the class of persons that Section 5 of the FTCA was intended to protect.

132. The harm occurring as a result of the Data Breach is the type of harm that Section 5 of the FTCA intended to guard against.

133. It was reasonably foreseeable to Rite Aid that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

134. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Rite Aid's violations of Section 5 of the FTCA. Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vi) actual or attempted fraud.

COUNT III
BREACH OF FIDUCIARY DUTY

135. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

136. Plaintiff and Class Members either directly or indirectly gave Rite Aid their PII in confidence, believing that Rite Aid would protect that information. Plaintiff and Class Members would not have provided Rite Aid with this information had they known it would not be adequately protected. Rite Aid's acceptance and storage of Plaintiff's and Class Members' PII created a

fiduciary relationship between Rite Aid and Plaintiff and Class Members. In light of this relationship, Rite Aid must act primarily for the benefit of its clients, which includes safeguarding and protecting Plaintiff's and Class Members' PII.

137. Rite Aid has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII, failing to comply with the data security guidelines set forth by Section 5 of the FTCA, and otherwise failing to safeguard the PII of Plaintiff and Class Members it collected.

138. As a direct and proximate result of Rite Aid's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII, which remains in Rite Aid's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT IV
BREACH OF IMPLIED CONTRACT

139. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

140. Defendant required Plaintiff and Class Members to provide, or authorize the transfer of, their PII in order for Rite Aid to provide services. In exchange, Defendant entered into implied contracts with Plaintiff and Class Members in which Defendant agreed to comply with its

statutory and common law duties to protect Plaintiff's and Class Members' PII and to timely notify them in the event of a data breach.

141. Plaintiff and Class Members would not have provided their PII to Defendant, or would not have agreed to have that information provided to Defendant, had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

142. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

143. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

144. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class Members.

COUNT V
UNJUST ENRICHMENT

145. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

146. This claim is pleaded in the alternative pursuant to Fed. R. Civ. P. 8(d).

147. Plaintiff and Class Members conferred a monetary benefit upon Rite Aid in the form of monies paid for debt collection services or other services.

148. Rite Aid accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Rite Aid also benefitted from the receipt of Plaintiff's and Class Members' PII.

149. As a result of Rite Aid's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

150. Rite Aid should not be permitted to retain the money belonging to Plaintiff and Class Members because Rite Aid failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws, and industry standards.

151. Rite Aid should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT VI
BREACH OF CONFIDENCE

152. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

153. Plaintiff and Class Members have an interest, both equitable and legal, in the PII about them that was conveyed or provided to, collected by, and maintained by Rite Aid, and that was ultimately accessed or compromised in the Data Breach.

154. Rite Aid has a special relationship to its clients and other affiliated persons, such as Plaintiff and the Class Members.

155. Because of that special relationship, Rite Aid was provided with and stored private and valuable PII related to Plaintiff and the Class, which it was required to maintain in confidence.

156. Plaintiff and the Class directly or indirectly provided Rite Aid with their PII under both the express and/or implied agreement of Rite Aid to limit the use and disclosure of such information.

157. Rite Aid owed a duty to Plaintiff and the Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

158. Rite Aid had an obligation to maintain the confidentiality of Plaintiff's and the Class Members' PII.

159. Plaintiff and the Class have a privacy interest in their personal matters, and Rite Aid had a duty not to disclose confidential information and records concerning its consumers, clients and employees.

160. As a result of the parties' relationship, Rite Aid had possession and knowledge of the confidential PII and confidential records of Plaintiff and the Class.

161. Plaintiff's and Class Members' PII is not generally known to the public and is confidential by nature.

162. Plaintiff and Class Members did not consent to nor authorize Rite Aid to release or disclose their PII to an unknown threat actor.

163. Rite Aid breached the duties of confidence it owed to Plaintiff and the Class when Plaintiff's and Class Members' PII was disclosed to unknown criminal hackers.

164. Rite Aid breached its duties of confidence by failing to safeguard PII, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information

that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) designing and implementing inadequate cybersecurity safeguards and controls; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to follow its own privacy policies and practices published to its consumers, clients and employees; (g) storing PII in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (h) making an unauthorized and unjustified disclosure and release of Plaintiff's and Class Members' PII to a criminal third party.

165. But for Rite Aid's wrongful breach of its duty of confidences owed to Plaintiff and the Class Members, their privacy, confidences, and PII would not have been compromised.

166. As a direct and proximate result of Rite Aid's breach of confidences, Plaintiff and the Class have suffered and/or are at a substantial increased risk of suffering injuries, including:

a. The erosion of the essential and confidential relationship between Rite Aid and Plaintiff and the Class.

b. Loss of the privacy and confidential nature of their PII;

c. Theft of their PII;

d. Costs associated with the detection and prevention of identity theft;

e. Costs associated with purchasing credit monitoring and identity theft protection services;

f. Lowered credit scores resulting from credit inquiries following fraudulent activities;

g. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

h. The imminent and certain impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

i. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Rite Aid with the mutual understanding that Rite Aid would safeguard PII against theft and not allow access and misuse of their data by others;

j. Continued risk of exposure to hackers and thieves of their PII, which remains in Rite Aid's possession and is subject to further breaches so long as Rite Aid fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

k. Loss of personal time spent carefully reviewing statements and accounts; and

l. Mental anguish accompanying the loss of confidences and disclosure of their confidential and private PII.

167. Additionally, Rite Aid received payments for services with the understanding that Rite Aid would uphold its responsibilities to maintain the confidences of Plaintiff's and Class Members' PII.

168. Rite Aid breached the confidence of Plaintiff and the Class Members when it made an unauthorized release and disclosure of their PII and, accordingly, it would be inequitable for Rite Aid to retain the benefit at Plaintiff's and Class Members' expense.

169. As a direct and proximate result of Rite Aid's breach of its duty, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT VII
DECLARATORY AND INJUNCTIVE RELIEF

170. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

171. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

172. Defendant owes a duty of care to Plaintiff and Class Members that require it to adequately secure Plaintiff's and Class Members' PII.

173. Defendant still possesses the PII of Plaintiff and Class Members.

174. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and Class Members.

175. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the

exposure of their PII and Defendant's failure to address the security failings that led to such exposure.

176. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

177. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any PII not necessary for its provision of services;

e. Ordering that Defendant conduct regular database scanning and security checks; and

f. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in their favor and against Rite Aid as follows:

A. Certifying the Class as requested herein, designating Plaintiff as class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, individually and on behalf of the Class, seeks appropriate injunctive relief designed to prevent Rite Aid from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft.

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: July 26, 2024

Respectfully submitted,

By: */s/ Kevin Laukaitis*
Kevin Laukaitis (PA Bar #321670)
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

SCIOLLA LAW FIRM, LLC
Andrew J. Sciolla (PA Bar #203445)
Land Title Building, Suite 1910
100 South Broad Street
Philadelphia, PA 19110
T: 267-328-5245
F: 215-972-1545
andrew@sciollalawfirm.com

Attorneys for Plaintiff and the Class